Exemple de configuration de caractéristique d'Automatique-reprise de vpc de Nexus 7000

Contenu

Introduction

Ce document décrit comment configurer la caractéristique virtuelle d'automatique-reprise de PortChannel (vpc) sur le Nexus 7000.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Pourquoi avons-nous besoin de l'Auo-reprise de vpc ?

Il y a deux principales raisons pour cette amélioration de vpc :

- Dans une panne ou une panne de courant de centre de traitement des données, les deux pairs de vpc qui sont composés des Commutateurs de Nexus 7000 ne sont pas en ligne. De temps en temps, seulement un des pairs peut être restauré. Puisque l'autre Nexus 7000 est toujours hors fonction, le vpc peer-link et le lien de pair-keepalive de vpc sont également hors fonction. Dans ce scénario, le vpc n'avance pas même pour le Nexus 7000 qui est déjà en fonction. Toutes les configurations de vpc doivent être retirées du Port canalisé sur ce Nexus 7000 pour faire fonctionner le Port canalisé. Quand l'autre Nexus 7000 avance, vous devez de nouveau apporter des modifications de configuration pour inclure la configuration de vpc pour tous les vpc. Dans la version 5.0(2) et ultérieures, vous pouvez configurer la commande de **restauration de recharge** sous la configuration de vpc domain d'aborder ce problème.
- Pour quelque raison, le vpc peer-link va hors fonction. Puisque la pair-keepalive de vpc est toujours en fonction, le périphérique secondaire de pair de vpc tourne tous ses ports membres de vpc outre d'en raison de la détection double-active. Par conséquent tout le trafic passe par le commutateur primaire de vpc. Pour quelque raison, le commutateur primaire de vpc va également hors fonction. Trous noirs de ce problème de commutateur le trafic puisque les vpc sur le périphérique secondaire de pair sont toujours hors fonction parce qu'il a détecté la détection double-active avant que le commutateur primaire de vpc soit allé hors fonction.

Dans la version 5.2(1) et ultérieures, la caractéristique d'automatique-reprise de vpc fusionne ces deux améliorations.

Configuration

La configuration de l'automatique-reprise de vpc est simple. Vous devez configurer l'automatique-reprise sous le vpc domain sur les deux pairs de vpc.

C'est un exemple de configuration :

Sur le commutateur S1

```
S1 (config)# vpc domain
S1(config-vpc-domain)# auto-recovery
S1# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 5
Peer Gateway                      : Enabled
Peer gateway excluded VLANs       : -
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)
```

```
vPC Peer-link status
--------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-112,114-120,800,810

vPC status
----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
10   Po40   up     success     success                    1-112,114-1
                                                         20,800,810
```

Sur le commutateur S2

```
S2 (config)# vpc domain 1
S2(config-vpc-domain)# auto-recovery
S2# show vpc
Legend:
              (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id                     : 1
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : secondary
Number of vPCs configured         : 5
Peer Gateway                      : Enabled
Peer gateway excluded VLANs       : -
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled (timeout = 240 seconds)

vPC Peer-link status
--------------------------------------------------------------------
id   Port   Status Active vlans
--   ----   ------ --------------------------------------------------
1    Po1    up     1-112,114-120,800,810

vPC status ----------------------------------------------------------------------
id   Port   Status Consistency Reason                     Active vlans
--   ----   ------ ----------- ------                     ------------
40   Po40   up     success     success                    1-112,114-1
                                                         20,800,810
```

Comment l'automatique-reprise fonctionne-t-elle vraiment ?

Cette section discute chaque comportement mentionné dans la section Informations générales séparément. La supposition est que l'automatique-reprise de vpc est configurée et enregistrée à la configuration de démarrage sur les Commutateurs S1 et le S2.

1. Une panne de courant a coupé des pairs de vpc de Nexus 7000 simultanément et seulement un commutateur peut avancer.
   - Le S1 et les S2 sont allumés tous deux. le vpc est formé correctement avec le pair-lien et la pair-keepalive en fonction.
   - Le S1 et les S2 mettent hors tension simultanément.
   - Maintenant seulement un commutateur peut mettre sous tension. Par exemple, S2 est le seul commutateur qui met sous tension.

- S2 attend le délai d'attente d'automatique-reprise de vpc (le par défaut est de 240 secondes qui peuvent être configurées avec la commande du recharge-**retard X d'automatique-reprise**, où **x** est de 240-3600 secondes) afin de vérifier si le vpc peer-link ou l'état de pair-keepalive met sous tension. Si l'un de ces liens est allumés (état de pair-lien ou de pair-keepalive), l'automatique-reprise n'est pas déclenchée.
- Après le délai d'attente, si les deux liens sont toujours hors fonction (état de pair-lien aussi bien que de pair-keepalive), les enables d'automatique-reprise de vpc et S2 devient primaire et initie afin de mettre sous tension son vpc local. Puisqu'il n'y a aucun pair, le contrôle de cohérence est sauté.
- Maintenant le S1 est livré en fonction. À ce moment, S2 retient son rôle primaire et le S1 joue un rôle secondaire, un contrôle de cohérence est exécuté, et des mesures appropriées sont prises.

2. le vpc peer-link met hors tension d'abord et alors le pair primaire de vpc met hors tension.
   - Le S1 et les S2 sont allumés tous deux et le vpc est formé correctement avec le pair-lien et la pair-keepalive en fonction.
   - Pour quelque raison, le vpc peer-link va hors fonction d'abord.
   - Puisque la pair-keepalive de vpc est toujours en fonction, elle détecte la détection double-active. Le vpc S2 secondaire arrête tous ses vpc locaux.
   - Maintenant le vpc S1 primaire va hors fonction ou des recharges.
   - Cette panne arrête également le lien de pair-keepalive de vpc.
   - S2 attend trois messages consécutifs de pair-keepalive à perdre. Pour quelque raison, ou le vpc peer-link avance ou S2 reçoit un message de pair-keepalive, et l'automatique-reprise n'active pas.
   - Cependant, si le pair-lien demeure hors fonction et trois messages consécutifs de pair-keepalive sont perdus, enables d'automatique-reprise de vpc.
   - S2 assume le rôle de primaire et active son vpc local qui saute le contrôle de cohérence.
   - Quand le S1 se termine la recharge, S2 retient son rôle de primaire et le S1 devient secondaire, un contrôle de cohérence est exécuté, et des mesures appropriées sont prises.

   Note: Comme expliqué dans les deux scénarios, le commutateur qui les unsuspends son rôle de vpc avec l'automatique-reprise de vpc continue à demeurer primaires même après que le pair-lien est allumé. L'autre pair joue le rôle de secondaire et interrompt son propre vpc jusqu'à ce qu'un contrôle de cohérence soit complet.

Exemple :

Le S1 est mis hors tension. S2 devient le primaire opérationnel comme prévu. le Pair-lien et la pair-keepalive et tous les liens de vpc sont déconnectés du S1. Le S1 n'est pas mis sous tension. Puisque le S1 est complètement isolé, il actionne le vpc sur (bien que les liens physiques sont en baisse) en raison de l'automatique-reprise et joue le rôle de primaire. Maintenant, si le pair-lien ou la pair-keepalive sont connectés entre le S1 et le S2, le S1 garde le rôle de primaire et S2 devient secondaire. Cette configuration fait interrompre S2 son vpc jusqu'à ce que le vpc peer-link et la pair-keepalive soient mis sous tension et le contrôle de cohérence est complet. Ce scénario entraîne le trafic au trou noir puisque le vpc S2 est secondaire et les liens S1 physiques sont éteints.

Est-ce que je devrais activer l'automatique-reprise de vpc ?

Automatique-reprise d'enable d'il est conseillé de dans votre environnement de vpc.

Il y a une légère occasion que la caractéristique d'automatique-reprise de vpc pourrait créer un scénario double-actif. Par exemple, si vous perdiez la première fois le pair-lien et alors vous perdiez la pair-keepalive, vous aurez le scénario double-actif.

Dans cette situation, chaque port membre de vpc continue à annoncer le même ID de Control Protocol d'agrégation de liaisons qu'il a fait avant la panne double-active.

Une topologie de vpc se protège intrinsèquement contre des boucles en cas de scénarios double-actifs. Dans un scénario de le pire des cas, il y a des trames en double. En dépit de ceci, comme mécanisme de boucle-prévention, Bridges Protocol Data Unit de chaque commutateur en avant (BPDU) avec le même ID de passerelle BPDU qu'avant la panne double-active de vpc.

Tandis que non intuitif, il est encore possible et desirable de continuer à expédier le trafic de la couche d'accès à la couche d'agrégation sans baisses pour la circulation en cours, à condition que les tables de Protocole ARP (Address Resolution Protocol) soient déjà remplies sur les deux pairs de gamme 7000 de Cisco Nexus pour tous les serveurs nécessaires.

Si de nouvelles adresses MAC doivent être apprises par la table ARP, les questions pourraient surgir. Les questions surgissent parce que la réponse d'ARP du serveur pourrait être hachée à un périphérique de gamme 7000 de Cisco Nexus et pas à l'autre, qui le rend impossible pour que le trafic circule correctement.

Supposez, cependant, qu'avant la panne dans la situation juste décrite, le trafic a été également distribué aux deux périphériques de gamme 7000 de Cisco Nexus par un PortChannel correct et par une configuration par trajets multiples de coût égal (ECMP). Dans ce cas, le trafic de serveur-à-serveur et de topologie continue la mise en garde qui simple-a relié des serveurs connectés directement à la gamme 7000 de Cisco Nexus ne pourra pas communiquer (pour le manque du lien de pair). En outre, de nouvelles adresses MAC apprises sur la gamme 7000 d'un Cisco Nexus ne peuvent pas être apprises sur le pair, parce que ceci entraînerait le trafic de retour qui arrive sur le périphérique de gamme 7000 de Cisco Nexus de pair pour inonder.

Référez-vous à la page 19 du Logiciel Cisco NX-OS PortChannel virtuel : Pour en savoir plus fondamental de concepts.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Support et documentation techniques - Cisco Systems